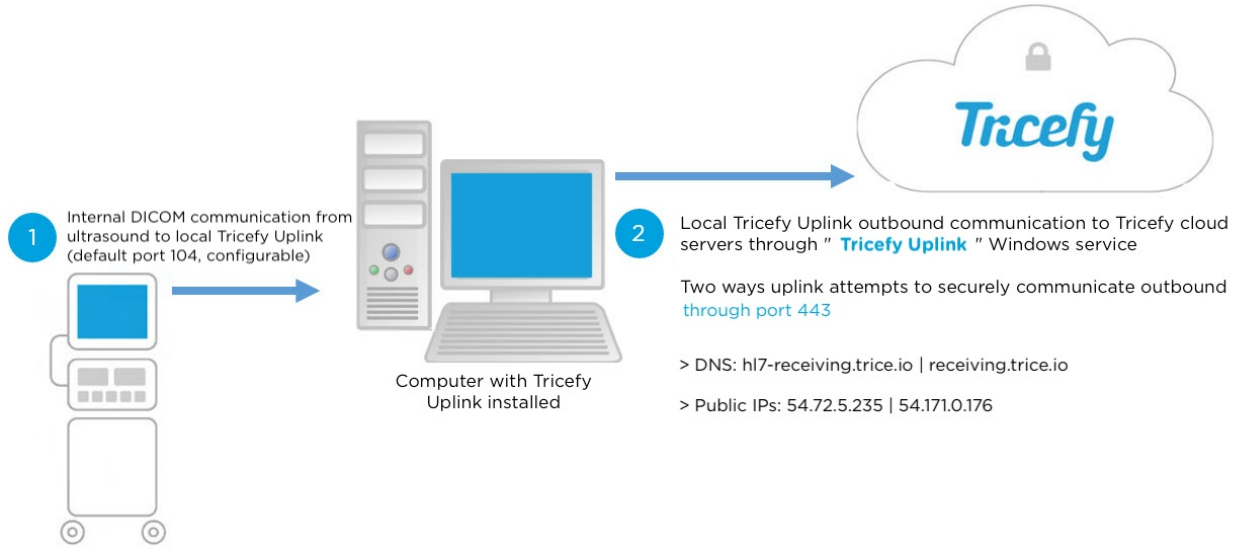
Network Setup and Firewalls

Last Modified on 2023-12-29 14:59



Destination IP Addresses and DNS

In some cases, firewall changes may be needed in order to allow the local Tricefy Uplink to communicate out to the Tricefy cloud -- usually whitelisting the IPs and/or domain uplink connects to.

Below is the Tricefy cloud domain and public IP addresses that the local Tricefy Uplink will attempt to reach the Tricefy cloud outbound via **port 443**:

hl7-receiving.trice.io

- 54.72.5.235
- 54.171.0.176

Note: legacy uplink will connect through a different domain (receiving.trice.io) but resolves to the same 2 public IPs above

---

Local Windows Firewall Settings

When Uplink is installed, a Windows service called – Tricefy Uplink – will run in the background. The installation process is designed to apply local Windows firewall rules to avoid from blocking the local uplink process/service, however a network firewall can still be blocking the traffic.

If you have an IT department, confirm with IT that firewalls are configured to allow the Tricefy Uplink process with the communication details above.

If you don't have an IT department, try the following troubleshooting steps:

- Temporarily turn off Windows firewall
  - Test the ultrasound connection using Ping/Verify - if it works, firewall needs to be configured to allow the Tricefy Uplink process
- Temporarily turn off anti-virus software
  - Test the ultrasound connection Ping/Verify - if it works, an AV software exception needs to be configured to allow the Tricefy Uplink process

---